Secure Coding

Lab – 9

Name :- A V puneeth

Reg.No :- 19BCN7041

Working with the memory vulnerabilities – Part III

Task

- Download Vulln.zip from teams.
- Deploy a virtual windows 7 instance and copy the Vulln.zip into it.
- Unzip the zip file. You will find two files named exploit.py and Vuln_Program_Stream.exe
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py) to generate the payload
- Install Vuln_Program_Stream.exe and Run the same

Analysis

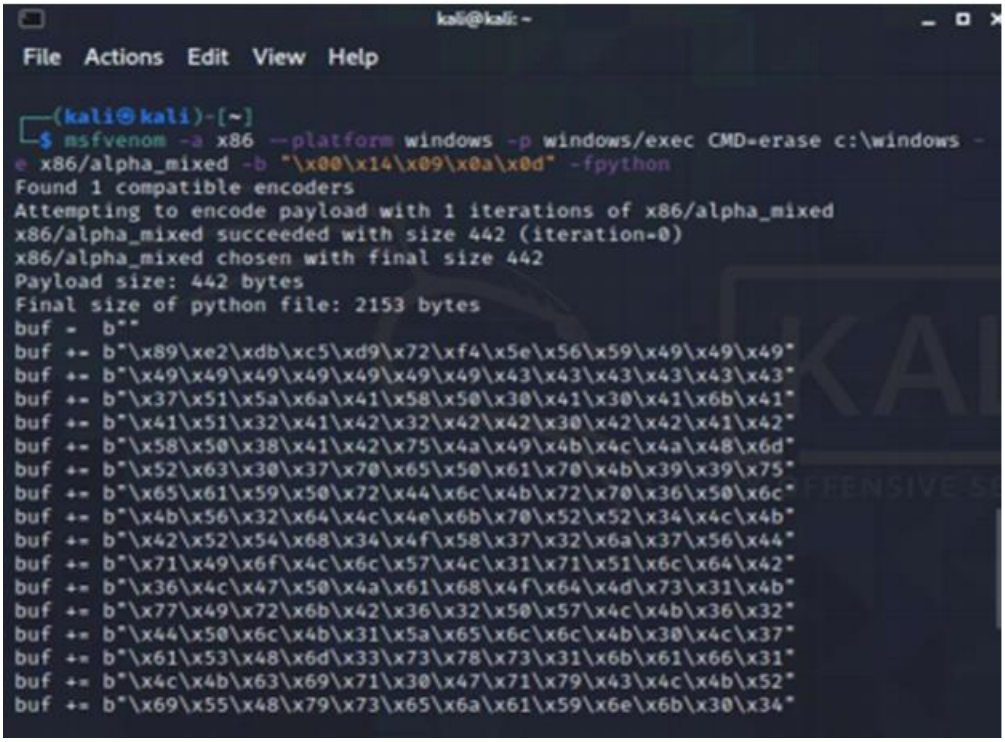
- Crash the Vuln_Program_Stream program and try to erase the hdd.
- First,we generate the payload using Kali Linux in VMWare to open the calculator and control panel in windows VM.
- Now that payload is attached in python file to write it into a text file.
- Use content of text file to exploit the program and open the designated applications.

Download and install kali linux using iso file in vmware workstation in your system

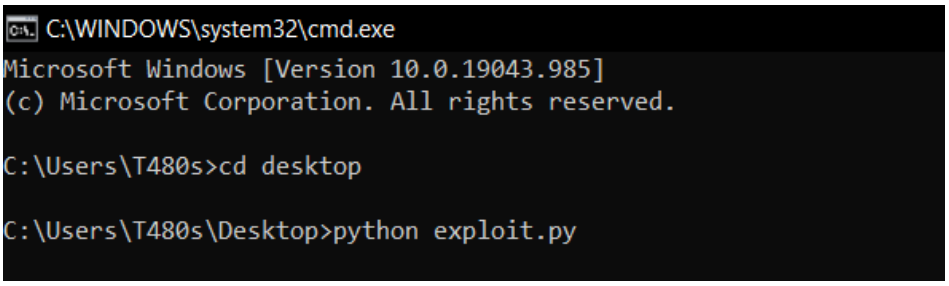
Download and install figrat application in windows 7 virtual machine.

For crash hdd:

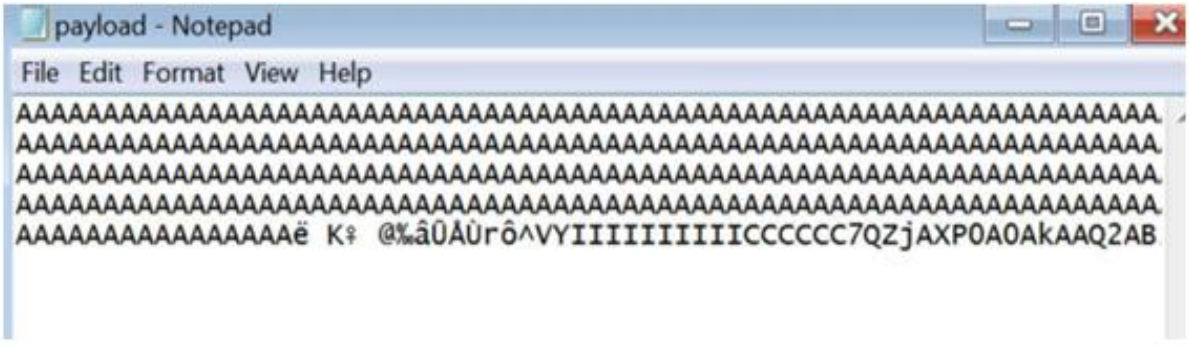
msfvenom -a x86 --platform windows -p windows/exec CMD=erase c:\windows -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python



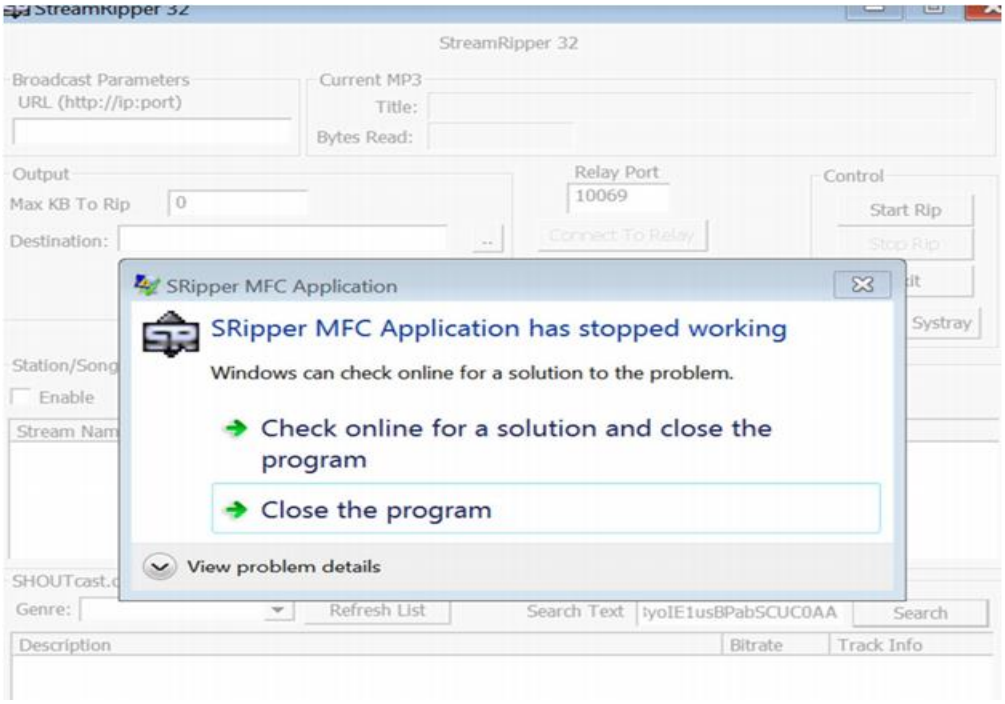
Generate payload by running exploit.py using cmd



Now payload will generate



Now open stream ripper and insert payload into it



Stream ripper crashes.

But the disk isn't cleared because of the security in windows 7 due to the security in windows 7 it doesn't allow formatting the drive when windows running, and also we created the shellcode for "/q" quite formatting, so we didn't get the sign of clearing the disk.